FORTINET

Application Control

Application control technologies detect and take action against network traffic based on the application that generated the traffic. Application control uses protocol decoders with signatures that analyze network traffic to detect application traffic, even if the traffic uses non-standard ports or protocols.

Enhance Control and Network Visbility

Controlling and monitoring applications on a network can seem like a daunting task due to the wide range of available applications. It is no longer an option to simply block or allow TCP and/or UDP ports since most applications do not map to individual ports. For example, controlling traffic on an HTTP or HTTPS port is futile against complex social networking sites and cloud applications.

FortiOS Application Control leverages its massive application database to identify applications and their activities while still providing a suitable and sufficient user experience, thanks to FortiASIC Content Processors (CPs), which boost CPU performance. Organizations can adopt more granular control, such as allowing logins but not chatting over selected sites. Traffic shaping may also be applied to the application traffic that is allowed. After applying control measures, continuous monitoring ensures that the measures are effective and allow for changes in application traffic patterns to be managed. For increased monitoring, unique deep visibility can also be enabled to reveal associated usernames and video/file information.

Key Features & Benefits

Identifies and controls application traffic.	Allows organization to strengthen security policies by controlling evasive application communications.
Leverages FortiGate's hardware acceleration and software optimization.	Offers more security without compromising performance..
Granular control and integration with other FortiOS capabilities.	Provides administrators the ability to implement the most appropriate configuration for any given organization.

Rich feature set for protecting your applications, data and users.

- Superior performance using the unique FortiASIC Content Processor that offloads heavy computation from the CPU
- Flexible implementation with robust deployment modes and granular controls
- Excellent visibility and management tools that help administrators improve security

NSS Labs "Recommend" Rating for Next Generation Firewall

Fortinet's entry into the NSS Labs Next Generation Firewall Group Test in 2013 & 2014 received the "Recommend" rating, placing it as one of the top performing systems. NSS Labs uses respectable real-world testing methodologies to measure Next Generation Firewall protection and performance, including application control.

Superior performance with Unique Hardware Architecture

Unlike a traditional security gateway, which relies heavily on CPUs for packet inspection, the FortiGate's unique hardware architecture allows FortiOS to automatically utilize appropriate hardware components to achieve optimal performance. This prevents the CPU from becoming a bottleneck as it performs various functions concurrently.

In support of application control, the Content Processor (CP) is a specialized ASIC chip that handles demanding cryptographic computation for SSL inspection and intensive signature matching. By offloading these processes from the CPU, the FortiGate is able to minimize performance degradation when administrators opt for greater security.

Robust Deployment Modes

FortiOS supports a wide array of network protocols and operating modes, allowing administrators to deploy the most appropriate security for their unique IT infrastructure. FortiOS also supports a variety of routing and switching protocols.

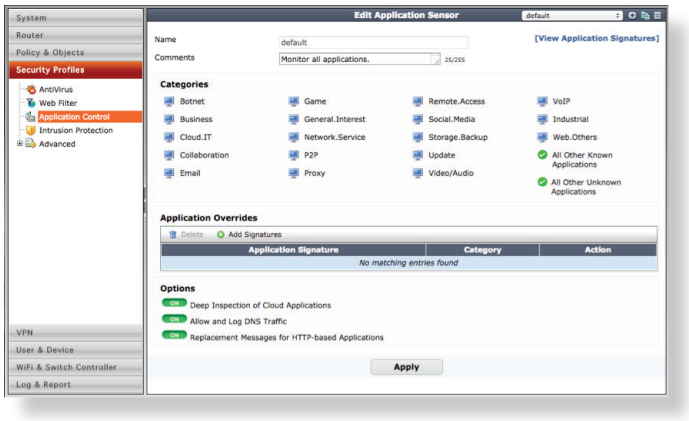
The FortiGate is able to operate in inline route and transparent mode. It can also operate in offline sniffer mode for passive monitoring of user activities. These different operating modes run concurrently by using virtual systems.

Advanced Application Detection and Control

By relying on the FortiOS 3rd Generation IPS engine, the FortiGate is able to inspect many of today's encrypted and evasive traffic, as well as traffic running on new technologies, such as SPDY protocol. The inspection can be applied to both network and IPsec/SSL VPN traffic.

An application and its specific activity are identified using FortiGuard's Application Control database of over 3,500 distinct signatures. These signatures are crafted by researchers across the globe to include applications that may be unique to platforms, regions, and/or languages. It also offers specific application activity identification, such as a Facebook posting or Dropbox file sync. The database is kept up to date via scheduled or manual downloads.

The application database is classified into 18 intuitive categories for ease of use. Administrators may also create specific application overrides that differ from the category settings. These specific applications can be filtered and selected by risk levels, technology type, and popularity.



Administrators may also apply advanced controls, such as setting up session TTLs for specific applications using CLI commands.

Traffic Shaping

Organizations may better utilize bandwidth and protect critical applications by enforcing granular application usage with traffic shaping. Administrators can create various traffic shaping profiles by defining traffic priority and maximum or guaranteed bandwidth. These profiles can then be assigned to targeted applications.

User Notification

User education is central to an effective security implementation. In response to this, FortiOS lets you provide user notification when blocking an unauthorized application. The notification appears as an HTML block page for web-based applications.

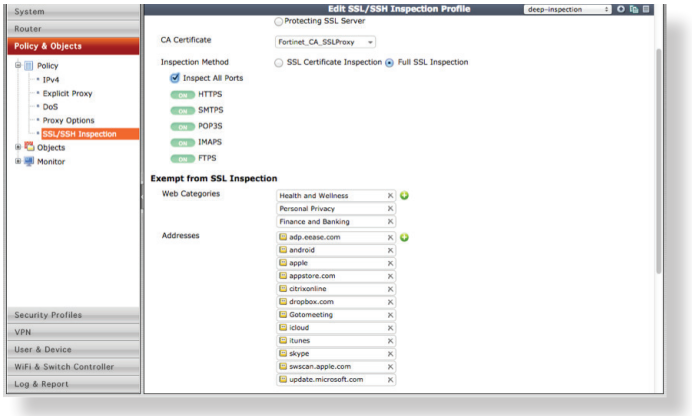
Advanced notification is possible by implementing Fortinet's

browser-embedded frame. And when “off-net” users are denied access, notifications appear via FortiClient’s notification pop-ups.

Deep Inspection for Cloud Applications

The prevalence of cloud applications like Dropbox poses a security challenge to today’s organizations. Using FortiOS’s deep inspection for cloud applications, administrators gain deep and useful insights, via FortiView and logs, into activities associated with these applications, such as user IDs, cloud actions, file names, and file sizes.

SSL Inspection for Encrypted Traffic



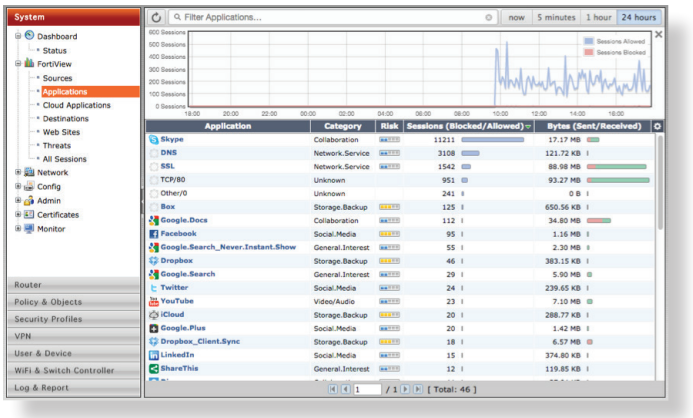
SSL (Secure Sockets Layer) is a popular encryption standard used to protect Internet traffic but may also be used to evade traditional inspection. FortiOS enables organizations to adopt effective application control even when traffic is encrypted.

Unique hardware components and software optimizations can decrypt traffic with minimal performance impact. The inspection can easily omit sensitive communications, such as financial transaction (thereby complying with privacy policies), or bypass applications that forbid SSL inspection by using granular policy settings.

Monitoring, Logging, and Reporting

FortiOS empowers organization to implement security best practices that require continuous examination of threat statuses and the ability to adapt to new requirements.

The FortiView online query widgets provide useful analyses with detailed and contextual session information that can



be filtered, ranked, and further inspected. For example, an administrator can instantly query the top applications that are currently consuming bandwidth and drill down to identify their users and help decide if such activities should be blocked.

FortiGate® - High performance Network Security Platform

- **ASIC-Powered Performance**
  FortiGate purpose-built hardware delivers unmatched price/performance for the most demanding networking environments. FortiASIC processors ensure that your network security solution does not become a network bottleneck.
- **High speed and Flexible Connectivity**
  The FortiGate product family offer a variety of interfaces for today’s network, ranging from integrated WAN interfaces, 3G/4G USB wireless broadband support to high speed 40G interfaces for data centers.
- **Broad Product Offerings**
  The FortiGate product family scales from desktop units for remote branch offices, mid-range for small and medium enterprises to high-end platforms for service providers and data centers

Network, threat, and system events activities can be archived via syslogs. In turn, these logs can generate useful trending and overview reports.

Lastly, the FortiOS offers robust in-built email and SMS alert systems. Meanwhile, integration with external threat management systems can be achieved with SNMP and standard-based syslogs.

ADDITIONAL REFERENCES

Resource	URL
The FortiOS Handbook - The Complete Guide	http://docs.fortinet.com/fgt.html
Fortinet Knowledge Base	http://kb.fortinet.com/
Product Datasheets & Matrix	http://www.fortinet.com/resource_center/datasheets.html
Fortinet Solution Page	http://www.fortinet.com/solutions

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
Fax: +1.408.235.7737

EMEA SALES OFFICE
120 rue Albert Caquot
06560, Sophia Antipolis,
France
Tel: +33.4.8987.0510
Fax: +33.4.8987.0501

APAC SALES OFFICE
300 Beach Road #20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730
Fax: +65.6223.6784

LATIN AMERICA SALES OFFICE
Prol. Paseo de la Reforma 115 Int. 702
Col. Lomas de Santa Fe,
C.P. 01219
Del. Alvaro Obregón
México D.F.
Tel: 011-52-(55) 5524-8480